Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 18 December 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The IDG News Service reports Cisco Systems Inc. is warning customers about security holes in its PIX firewall product and firewall software that runs on the Catalyst 6500 Series and 7600 Series switches. (See item 23)
- vnunet reports security experts have warned that hackers are preparing Christmas card emails that appear to lead to innocent images, but in fact trick users with Windows systems into downloading viruses. (See item 24)
- Global Security Newswire reports Indian police in the Jammu and Kashmir region have discovered a small pistol with 25 bullets that may have been coated in a lethal chemical agent. (See item 28)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *December 18, Federal Energy Regulatory Commission* — **Expansion needed for New England natural gas infrastructure to meet future demands.** The Federal Energy Regulatory Commission (FERC) Wednesday, December 17, released a study prepared in consultation with the Department of Energy that concludes **there is adequate natural gas infrastructure to meet demand through 2005, but additional infrastructure will be needed**

to meet New England's demand for natural gas through 2010. There are no native sources of natural gas or underground storage facilities in New England. The region currently depends on interstate natural gas pipelines, imported liquefied natural gas (LNG) and very limited above−ground storage of LNG to meet demand. During peak periods of demand, the interstate pipeline system is operated at a very high load factor and is not able to fully access underground storage in New York and Pennsylvania. **Construction of new pipeline capacity to these storage facilities and to expanded or newly constructed LNG import facilities would enhance New England's natural gas infrastructure**, the study notes. The study is available online: http://www.ferc.gov/EventCalendar/Files/20031217114525−A−3−p ublic.pdf
Source: http://www.ferc.gov/press−room/pr−current/12−17−03.asp

2. *December 17, Associated Press* — **Crude oil inventories low. U.S. commercial crude oil inventories fell 5.1 million barrels, or 1.8 percent, to 272.8 million barrels in the week ended December 12, amid a drop in crude oil imports**, the Department of Energy (DOE) reported Wednesday, December 17. **That sets a new low for December oil stocks since the Energy Information Administration (EIA), the statistical branch of the DOE, began collecting inventory data in 1982**. The decline greatly exceeded expectations, as analysts surveyed earlier this week by Dow Jones Newswires had expected a draw in crude inventories of only 1.5 million barrels. In the last four reporting weeks, crude inventories have posted heavy draws totaling 21.2 million barrels, according to the EIA. U.S. crude oil imports averaged above 9.1 million barrels a day last week, down 391,000 barrels a day from the prior week, with the West Coast accounting for most of the decline.
Source: http://www.nytimes.com/aponline/business/AP−Oil−Prices.html

3. *December 17, Federal Energy Regulatory Commission* — **FERC to require reporting of power−grid reliability violations. The Federal Energy Regulatory Commission (FERC) Wednesday, December 17, directed staff to develop an order that will require transmission system operators to report violations of the industry's power−grid reliability standards**. The pending order marks the first step in the Commission's exploration of its authority under existing law to assure power grid reliability in the aftermath of an August 14, 2003, blackout that affected millions in the U.S. and Canada. In approving the staff's recommendation, the four sitting FERC members agreed that the Commission would continue to explore what additional measures it can take under its existing statutory authority. The Commission is inviting public comment on the extent to which it can address grid reliability under existing law. Comments should be filed in Docket No. AD02−7.
Source: http://www.ferc.gov/press−room/pr−current/12−17−03−3.asp

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *December 16, Honolulu Advertiser* — **Stryker brigade is approved for Hawaii.** Secretary of Defense Donald Rumsfeld has approved a rapid−response Stryker Brigade Combat Team for Hawaii that will include increased firepower from the ground and air. **The Stryker Brigade is expected to be operational in 2007, equipped with new lightweight 155 mm howitzers and new Comanche helicopters, scheduled to be in service in 2009**. The Stryker will be the 2nd Brigade of the 25th Infantry Division (Light) and be based at Schofield Barracks. **The Stryker is key to the Pentagon's goal of remaking the Army into a more versatile force that can move quickly to distant battlefields**. The units, built around the 20−ton, eight−wheeled Stryker vehicle, are far quicker than a traditional armored unit centered around the tank. The first Stryker is in Iraq, accompanied by an aviation battalion task force comprised of OH−58 Kiowa Warriors and UH−60 Black Hawk helicopters, according to the "Inside the Army" newsletter.
   Source: http://the.honoluluadvertiser.com/article/2003/Dec/16/ln/ln0 1Abercrombiea.html

[Return to top]

Banking and Finance Sector

5. *December 16, British Bankers Association* — **New qualification strengthens fight against money laundering.** A new qualification designed to recognize professional standards in money laundering prevention has been launched by the British Bankers' Association (BBA) in partnership with the International Compliance Association (ICA) and the University of Manchester Business School in the UK. **As well as providing employers with the assurance that they are employing a properly trained individual in what has become a vitally important role, the Diploma in Anti Money Laundering, Dip (AML), will also provide Money Laundering Reporting Officers and others carrying out similar functions with clear evidence of professional competence**. An alternative qualification of Certificate in Anti Money Laundering Awareness is also available. This is aimed at all staff whose employment requires them to understand the threats posed to financial services business by criminally derived property.
   Source: http://www.btnsn.com/btnsn/pr_view.asp?id=4927&cid=8415

[Return to top]

Transportation Sector

6. *December 17, Newsday (Long Island, NY)* — **Commuters give LIRR C+.** In the annual Long Island Rail Road (LIRR) Report Card that looks at everything from on−time performance to bathroom cleanliness, riders gave the railroad a C+ −− the same grade they have assigned since 2000. However, statistically, **the railroad's score has dropped showing that riders are less confident that the railroad is improving. "I think it had a lot to do with the fare raise," said James McGovern, chair of the LIRR Commuter's Council, the group that issues the report card. "With more money, people are expecting better service."** The report details the results of a survey taken in July of 1,278 LIRR riders who were asked to grade the railroad's performance. Receiving the lowest score of a D+ were the restrooms at the Flatbush Terminal and those aboard the LIRR trains. **Out of a list of five possible service improvements, riders**

ranked better on−time performance and more frequent peak and off−peak service as top priorities. Waiting at the Hicksville station this morning, sometime rider Rhason Burke called the score "fair." "On−time, it's usually good," he said. "As for cleanliness, that's good also. The train is definitely quicker than the bus."
Source: http://www.newsday.com/news/local/longisland/ny−lirrreportcard1217,0,7947541.story?coll=ny−top−headlines

7. *December 17, Associated Press* — **DIA to test surveillance system.** The Transportation Security Administration has announced a $310,000 test of an advanced video surveillance system at Denver's airport, a part of a series of security upgrades at airports nationwide that will cost $7.8 million. **Denver International Airport (DIA) spokesman Steve Snyder said the facility's money will be used in part to install new digital technology that should improve the images from video cameras around the airport.** In August 2002, there was a security breach at DIA when a woman slipped out of a screening line at a security checkpoint and walked undetected to an airport train. The incident prompted the re−screening of as many as 15,000 passengers, officials said. Investigators had video images of the woman, but they complained that the film was so grainy it was difficult to identify her, and she never was located. **The new technology DIA will test should help security officials link images from different cameras so someone who triggers a security breach could be followed, Snyder said.** The money is coming as a "cooperative research agreement" with the Federal Aviation Administration, although officials declined to say when the technology would be operational.
Source: http://news4colorado.com/localnews/local_story_351115707.html

8. *December 17, Associated Press* — **New "smart" highways could warn drivers of trouble.** Federal regulators approved a step Wednesday toward developing smart highways, where warning signals automatically transmitted to drivers can prevent traffic accidents. **The Federal Communications Commission (FCC) set aside an area of broadcast spectrum to transmit those signals, rather than have them share space with electronic toll sensors, cell phones and garage door openers. "Smart radio technology means smarter highways, safer roads and a more secure homeland," FCC Chairman Michael Powell said.** Transportation Department officials are testing the technology at an intersection in McLean, VA, where sensors can automatically warn a motorist when another car is approaching, thus helping to avoid a collision. The technology, still five to 10 years away from being installed in cars and along highways, also could use a beep, a dashboard light or an electronic voice to tell drivers when it's safe to change lanes, or when to put on the breaks to avoid rear−ending the motorist in front.
Source: http://www.cnn.com/2003/TECH/ptech/12/17/smart.highway.ap/index.html

9. *December 17, The Press−Tribune (Roseville, CA)* — **Train derailment in Roseville.** A Union Pacific train heading into Roseville, CA, derailed near Thunder Valley Casino Tuesday at 8:06 a.m., halting traffic as response teams worked to secure the site and deal with potential hazards of the incident. The 86−car train, inbound to Roseville from Portland, derailed at Industrial and Athens avenues, spilling 28 cars off the tracks. **The cars were carrying lumber and plastic pellets, plus an empty container that had previously contained chemicals, said Mark Davis, Union Pacific spokesman.** No one was injured in the accident. Response teams from the railroad, city, county and regional agencies worked to secure the area while addressing hazards of a minor chemical leak from one vessel, and checking underground gas pipes for

potential damage. Jim Farmer of Roseville Union Pacific says 50 personnel were on site as well as 15 pieces of heavy equipment. Crews removed the 58 cars that remained on the track from the site. They were using heavy equipment movers to remove the derailed vessels. Cleanup should be finished today by noon, Farmer said. **The container carrying benzene chloride was ruptured and apparently was under some pressure. It was leaking out, but eventually the pressure stabilized and the leak stopped.** A common risk with train derailments are underground fuel lines that can be punctured when cars derail.
Source: http://www.thepresstribune.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=3754

[Return to top]

Postal and Shipping Sector

10. *December 17, Bangkok Post* — **DHL to undergo major expansion plan. DHL, the world's leading air delivery and logistics provider, plans to boost its Thai operations with major capacity expansion of its depots nationwide and the construction of a new warehouse and distribution centers.** Herbert Vongpusanachai, managing director of DHL Express, said the company's capacity would be more than doubled to serve business expansion over the next five to 10 years. Presently, the available capacity at its depots in Bangkok, Phuket, and Nakhon Ratchasima are almost fully utilized. The company expects to handle more than 130,000 tons of goods sent this year in express, air and ocean freight. The Thai expansion plans for next year follows the recent opening of Thailand's largest air express facility at Don Muang International Airport and seven new service facilities. DHL is the biggest air express provider in Thailand, holding more than 50 percent of the market in terms of shipments. Other major players are TNT Express, FedEx, and UPS.
Source: http://www.bangkokpost.com/Business/18Dec2003_biz76.html

[Return to top]

Agriculture Sector

11. *December 16, Associated Press* — **Brucellosis−infected cattle had been vaccinated. All 31 cattle which tested positive for brucellosis on a ranch in the Boulder, WY, area had been vaccinated against the disease, according to a U.S. Department of Agriculture (USDA) veterinarian.** Bret Combs, a veterinarian with the USDA's Animal and Plant Health Inspection Service, said Tuesday that seven of the infected cattle had been inoculated with the Strain 19 vaccine and the rest with the newer RB51 vaccine, which began being administered around 1996. Although it is impossible to tell how many cattle were exposed to Brucellosis bacteria, testing revealed the disease in about eight percent of the 391 cattle on Donald Jensen's herd. "All the data that we have shows that Strain 19 and RB51, as far as efficacy, they're pretty much equal," Combs said. "You're probably looking at somewhere between the low to mid 70 percent range." State law requires cows over a year old to have been given the brucellosis vaccine as calves before they can change ownership. Testing so far has not revealed brucellosis in a second herd, which would cost Wyoming its federal brucellosis−free status.
Source: http://www.trib.com/AP/wire_detail.php?wire_num=17368

12. *December 15, Western Producer* — **Fungal disease appears first time in Canada. A harvest survey found the disease club root in more than a dozen widely separated canola fields around Edmonton, Canada, this year.** Club root is a fungus that infects plants in the cole family, such as cabbage, turnips, and rutabaga. Canola is also in the family. Although the disease is a problem in vegetable crops in Ontario and British Columbia, Canada, it had not been observed in prairie canola crops. The fungus causes galls to form on the plant's roots. They restrict water and nutrients from getting to the rest of the plant, stunting growth, causing wilt, and reducing yield. The disease is a problem in oilseed rape in northern Europe, and the experience there may illustrate potential yield loss. **In Europe, a 100 percent infection can reduce yield by 50 to 80 percent. At an infection level of 10 to 20 percent, damage of five to 10 percent is common.** Fungicides are used on high value crops such as cabbage, but the same application method would be uneconomical for canola. The spores can persist in the soil for many years. Swedish research found that when a field was infested with club root, it took 17 years for it to go down to a non−detectable level in a bio−assay, and it had a 31/2 year half life.
Source: http://www.producer.com/articles/20031211/production/2003121 1prod02.html

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

13. *December 17, Inland Valley Daily Bulletin* — **Improving water supply after wildfires to cost $450 million.** Restoring and protecting the Santa Ana River watershed, in California, from the effects of October and November's wildfires could cost nearly $450 million, according to a report from Santa Ana Watershed Project Authority, whose members include regional water districts. **While the Project Authority's report is preliminary, some Inland Valley water agencies said they are already incurring added costs from the fires' effects. Ash and soot from the wildfires is affecting the water supply of Cucamonga County Water District, which has been unable to use water from four area canyons.** It's unknown how long it will be until the water district can use the canyon water, said Jo Lynne Pereyra, assistant to the general manager. The wildfires may also affect Inland Valley basins used to store water if heavy rains come. **Rain washing down bare hillsides is expected to bring more sediment and silt into the lower Inland Valley, filling basins that are used to percolate water into the Chino groundwater basin, an underground, nearly valleywide basin from which cities and water districts draw water.** But heavy sediment and silt from the hillsides could seal the basins, preventing water from percolating underground.
Source: http://www.dailybulletin.com/Stories/0,1413,203%257E24821%25 7E1835050,00.html

[Return to top]

Public Health Sector

14. *December 17, News.com Australia* — **SARS strikes again in Taiwan. A medical researcher in a Taiwan has tested positive for Severe Acute Respiratory Syndrome (SARS).** The patient is a man who had been studying SARS at the National Defense University, according to a news release issued by Taiwan's Center for Disease Control. The researcher attended a conference in Singapore on December 7 and developed a fever on December 10 after returning to Taiwan, officials said. Singapore reported a similar case last September when a Singaporean lab worker caught SARS while researching the illness. During the SARS outbreak earlier this year, Taiwan ranked third highest in the world behind China and Hong Kong for SARS deaths and cases.
Source: http://www.news.com.au/common/story_page/0,4057,8191134%255E 2,00.html

15. *December 16, University of Michigan Health System* — **Scientists discover how anthrax creates its deadly spores.** Spores of Bacillus anthracis, the bacterium that causes anthrax, can survive drought, bitter cold, and other harsh conditions for decades, yet still germinate almost instantly to infect and kill once inside an animal or human host. In a collaboration funded by the U.S. Office of Naval Research and the National Institutes of Health, scientists from three major research institutions, the University of Michigan, The Institute for Genomic Research, and The Scripps Research Institute, are working together to identify the genes and proteins involved in anthrax's deadly metamorphosis. **Their work provides information other researchers can use to develop new vaccines and treatments targeted at specific points in the complex process of anthrax growth and spore formation.** This study is the first analysis of a bacterial pathogen using the combined investigative tools of genomics and proteomics. It is also the first study to document, at a molecular level, all the genes and proteins involved in Bacillus anthracis spore formation. Major findings of the study include: **When compared to other bacteria, anthrax spore formation is an unusually complex and intricate process. Up to one−third of all the genes in the Bacillus anthracis genome are involved in spore production.**
Source: http://www.eurekalert.org/pub_releases/2003−12/uomh−sdh12110 3.php

16. *December 16, Reuters* — **Flu vaccine shortage highlights vaccine woes.** The current run on influenza shots in the U.S. highlights the neglected status of vaccines, health experts said on Tuesday. **Officials from the Department of Health and Human Services and the Food and Drug Administration said they hoped $50 million allocated by Congress to improve flu vaccine production in 2004 will help by next autumn's flu season, and promised to speed up changes aimed at making the system more nimble.** It will be spent to buy eggs to produce the current vaccine, and to encourage companies to take up new production methods that do not rely on eggs. The virus does not always grow perfectly in the eggs, so it is an unpredictable process. In a report published Wednesday, the National Vaccine Advisory Committee recommended increased government funding for vaccine stockpiles. **The committee said sporadic shortages of vaccines routinely given to children for mumps, measles, and other diseases are likely to continue unless some changes are made. It advised stronger liability protections for manufacturers; a requirement that manufacturers give advance notice if they are leaving the marketplace; and a national campaign to emphasize the safety and benefits of vaccines.**
Source: http://story.news.yahoo.com/news?tmpl=story&cid=571&ncid=751 &e=9&u=/nm/20031216/hl_nm/health_vaccines_dc

17. *December 15, CIDRAP* — **HHS sets rules for smallpox vaccine injury compensation.** The Department of Health and Human Services (HHS) has announced details of how the compensation program for civilians who are injured by the smallpox vaccine will work. **The $42 million program is intended to provide financial and medical benefits to people who suffer complications from a smallpox shot given under an HHS−approved smallpox emergency response plan. The program also is designed to help unvaccinated people who are harmed as a result of contact with vaccinees.** Almost 39,000 healthcare, public health, and emergency workers have received shots since the civilian smallpox vaccination program began last January. HHS Secretary Tommy Thompson announced on December 12 an interim rule that describes program eligibility standards, the process for requesting and receiving benefits, and other policies and procedures.
Source: http://www.cidrap.umn.edu/cidrap/content/bt/smallpox/news/de c1503vaccine.html

[Return to top]

Government Sector

18. *December 17, BizReport* — **U.S. considers expanding FBI database.** Homeland security officials want to add tens of thousands of illegal immigrants and foreign students to an FBI database designed primarily to help police apprehend wanted criminals, allowing them to instantly identify foreign nationals who have been deported or have violated student visas. The proposal is raising concerns among some civil liberties advocates and law enforcement groups that fear it will bring police heavily into the business of apprehending immigration violators who have committed no serious crimes. **Under the proposal, the FBI's main fugitive database would be expanded to include the names of 140,000 immigrants who are deported each year for noncriminal reasons, officials said.** An unknown number return to the country and are here illegally. Authorities also would add the names of thousands of foreign students who do not show up for class or otherwise violate their visas. **The FBI's database, known as the National Crime Information Center (NCIC), includes the names of more than 40 million felons, fugitives, missing persons and others being sought by law enforcement agencies. It is used by more than 80,000 law enforcement agencies.**
Source: http://www.bizreport.com/article.php?art_id=5766

[Return to top]

Emergency Services Sector

19. *December 17, The Hawk Eye (Burlington, IA)* — **Santa Fe bridge attack drill set for January.** Federal officials will study the probable effects of a terrorist attack on the Santa Fe Bridge next month, according to Lee County (Iowa) Emergency Management officials. Steve Cirinna, the county's emergency management coordinator, said the Homeland Security Department, Transportation Security Administration, Lee County, Fort Madison and Burlington Northern Santa Fe railroad officials will be presented with scenarios related to an attack on the bridge in Newport, RI, the last week of January. **The bridge, which carries thousands of tons of rail freight each day as well as hundreds of motor vehicles, was put on 24–hour watch**

in March after it was deemed one of 250 "critical assets" by the Homeland Security Department.
Source: http://www.thehawkeye.com/daily/stories/ln2_1217.html

20. *December 17, Newswise* — **Emergency responders to benefit from new bio−containment systems.** Jacksonville, FL, Fire/Rescue Hazmat Lieutenant Rick Rochford hopes he has seen the last of the days when a response call to a tractor−trailer spill on the interstate, or a leak at a nearby factory, is affected by improper equipment or procedures that taint test results and potentially put people in harm's way. **"Our department currently responds to about 300−500 Hazmat calls a year," says Rochford, also an instructor in chemical and biological sampling techniques. Now, Rochford and other emergency responders focused on protecting themselves and the general public, while at the same time maintaining evidence at the scene, have a new "weapon" — the Bio−Containment System — on their side.** "We needed a kit that is as simple as possible for a responder to go to the scene and collect, package, decontaminate and send for testing a sample of a potential biological agent," Rochford says. "Response to incidents that may involve biological agents has become an important aspect of the emergency responder's mission. In the past, there have been no set procedures to do this. The Bio−Containment System is the total solution that addresses these challenges."
Source: http://www.newswise.com/articles/view/502529/

[Return to top]

Information and Telecommunications Sector

21. *December 17, Government Computer News* — **Senate considers bill to limit peer−to−peer security risks.** A bill requiring federal agencies to curb the security risks caused by peer−to−peer file sharing is scheduled to go to the floor of the Senate next year. **HR 3159, the Government Network Security Act of 2003, would require agencies to develop and implement plans for protecting federal systems from the security and privacy risks posed by peer−to−peer file sharing. It also would require the General Accounting Office to assess the plans' effectiveness**. The House passed HR 3159 on October 8. The Senate Governmental Affairs Committee approved the legislation without amendment November 10, clearing the way for floor consideration of the bill. Because the Senate and House versions of the bill are identical, there would be no need for a conference committee to resolve differences. **The House committee said in a fact sheet on the bill that it had found peer−to−peer file sharing at federal agencies that use classified data, such as an Energy Department laboratory, a NASA research facility and Labor Department headquarters**.
Source: http://www.gcn.com/vol1_no1/daily−updates/24468−1.html

22. *December 17, Washington Post* — **2003 worst year ever for cybersecurity.** The year 2003 has been one of the worst years ever for cybersecurity, as hackers and spammers repeatedly demonstrated just how easy it is to use the latest software security holes, worms and viruses to attack businesses and trick Internet users into divulging their personal and financial information. And 2004 could be worse. "Bogus e−mails [are] quickly becoming more and more complex and sophisticated," said Johannes Ullrich of the SANS Internet Storm Center. "It's becoming harder to distinguish between what's real and what's fake." **A big trend in 2003 has**

been the growing number of malicious programs unleashed on the Internet that can give hackers control over an infected computer, a problem fueled by the proliferation of unsecured broadband connections that make it possible for hackers to gain access to thousands of machines with the release of one virus or worm. The success of these viruses has spawned a whole new illegal marketplace, as criminals pay hard cash for lists of infected computers. Even as criminals can exploit a whole list of newly discovered vulnerabilities, Ullrich said he expects a bumper crop of new computers to be infected with old worms and viruses still circulating on the Internet as millions of consumers plug in shiny new computers they receive over the holidays.
Source: http://www.washingtonpost.com/wp−dyn/articles/A5934−2003Dec1 6.html

23. *December 16, IDG News Service* — **Cisco warns of holes in PIX firewalls.** Cisco issued two security advisories on Monday, December 15. **Certain versions of the PIX firewall can be crashed and restarted in a denial of service (DoS) attack when they receive messages using the SNMP version 3 (SNMPv3) protocol**. An SNMP server must be defined for the Cisco firewall in order for SNMPv3 attack to succeed, Cisco said: http://www.cisco.com/warp/public/707/cisco−sa−20031215−pix.s html. Catalyst switches running the Cisco Firewall Services Module (FWSM) are also vulnerable to DoS attacks using SNMPv3. **A buffer overflow vulnerability discovered in the FWSM could allow a malicious hacker using either RADIUS (Remote Authentication Dial−In User Service) or TACACS+ (Terminal Access Controller Access Control System) to crash a Cisco firewall with a user authentication request sent using HTTP**, Cisco said: http://www.cisco.com/warp/public/707/cisco−sa−20031215−fwsm. shtml. PIX firewalls running software versions 6.3.1, 6.2.2 and earlier, version 6.1.4 and earlier and version 5.x.x and earlier are all vulnerable to the SNMPv3 security hole, as are Catalyst 6500 and 7600 series switches running FWSM software up to and including version 1.1.2. Catalyst switches running FWSM software up to and including version 1.1.2 are also vulnerable to the HTTP authentication vulnerability.
Source: http://www.infoworld.com/article/03/12/16/HNciscopix_1.html

24. *December 15, vnunet.com* — **Christmas virus on the cards.** Security experts last week warned that **hackers are preparing Christmas card emails that appear to lead to innocent images, but in fact trick users with Windows systems into downloading viruses**. Security specialist ISS said **contributors to hacker mailing lists have recently been discussing new techniques to bypass firewalls by mislabelling general HTML files as JPEGs**. Steven Darrall of ISS said the problem is caused by Microsoft's Internet Explorer (IE) web browser automatically opening files labelled with .jpg or .gif extensions. Hackers have posted a proof−of−concept file in which the content was a script that caused the browser to download and install a virus, Darrall said. The site serving the virus has since been shut down, but Darrall warned that the online discussions could be the first sign of trouble ahead.
Source: http://www.vnunet.com/News/1151553

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 17300 (Kuang2TheVirus), 445 (microsoft−ds), 53 (domain), 80 (www), 23 (telnet), 1433 (ms−sql−s), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

25. *December 17, U.S. Department of State* — **Travel Warning: Saudi Arabia.** Due to ongoing security concerns, on December 17, the Department of State warned U.S. citizens to defer travel to Saudi Arabia and authorized the departure, on a voluntary basis, of family members and non−emergency personnel of the U.S. Embassy and Consulates in Saudi Arabia. **The U.S. Government continues to receive indications of terrorist threats aimed at American and Western interests, including the targeting of transportation and civil aviation**. American citizens in Saudi Arabia should remain vigilant, particularly in public places associated with the Western community. Terrorists have attacked residential housing compounds in the Riyadh area in 2003. **Credible information indicates that terrorists continue to target residential compounds in Saudi Arabia, particularly in the Riyadh area, but also compounds throughout the country**.
Source: http://travel.state.gov/saudi_warning.html

26. *December 17, Washington Post* — **Hussein document exposes network. A document discovered during the capture of former Iraqi president Saddam Hussein has enabled U.S. military authorities to assemble detailed knowledge of a key network behind as many as 14 clandestine insurgent cells, a senior U.S. military officer said Tuesday.** "I think this network that sits over the cells was clearly responsible for financing of the cells, and we think we're into that network," said Army Brig. Gen. Martin E. Dempsey, commander of the 1st Armored Division. **Acting quickly after realizing the significance of the document, troops of the 1st Armored Division conducted raids Sunday and Monday that netted three former Iraqi generals suspected of financing and guiding insurgent operations in the Baghdad area.** Dempsey declined to name the three officers who were detained. He said none was on the Pentagon's list of the 55 most wanted Iraqis but said their family names were familiar to U.S. authorities, suggesting that relatives of the men had come under suspicion.

Other Iraqis cited in the document are still being sought, the general added. Dempsey said other documents found with Hussein could end up exposing other enemy networks.
Source: http://www.washingtonpost.com/wp−dyn/articles/A6165−2003Dec1 6.html

27. *December 17, Associated Press* — **Storm blankets part of U.S. with snow.** A storm blanketed parts of the northeastern United States with heavy snow and slush Monday, just a week after another snowstorm pounded the region. **At least seven deaths were blamed on the storm and scattered school closings were reported from North Carolina to Maine. Some flights were canceled or delayed at Boston's Logan International Airport, spokesman Phil Orlandella said. Portland International Jetport in Maine also had delays and cancellations.** The heaviest snowfall was in northern Vermont, where the Jay Peak ski area recorded 38 inches by Monday morning. As much as 18 inches of snow had fallen at Syracuse, New York, with 13 inches in parts of Maine and New Hampshire. The storm −− called a nor'easter for the circulation that brings wind blowing in off the ocean −− had moved up the East Coast and Appalachians, soaking parts of the Carolinas and dropping 10 inches of snow in the mountains of West Virginia, before reaching New England on Sunday. The storm blacked out some 14,000 customers in Springfield, Massachusetts, Monday morning, Western Massachusetts Electric Co. reported. Power had been restored to about 16,000 customers who were blacked out by the storm in North Carolina, utilities said.
Source: http://www.fema.gov/press/ap/ap121603.shtm

28. *December 15, Global Security Newswire* — **Indian police discover possible chemical pistol.** Indian police in the Jammu and Kashmir region have discovered a small pistol with 25 bullets that may have been coated in a lethal chemical agent, police officials said Saturday, December 14. **“We recovered a pen−pistol and 25 cartridges. When one of our men tried to remove the cartridge inside, it emitted fumes and he felt dizzy and became unconscious,”** said K. Rajendra, inspector general of police in the region. “We have sent the pistol and bullets for forensic examination. Initial tests reveal the bullets are laced with a neurotoxic substance,” Rajendra added. The weapon was found last week in a house near the border with Pakistan, according to Rajendra. The owner of the house is currently being held. **The cartridges were reportedly marked “Neuroxin” and “BA,”** according to police.
Source: http://www.nti.org/d_newswire/issues/2003/12/15/2ebae4ae−ef1 6−4793−95ff−85528e0450b9.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer